### No. 18-16700

# IN THE UNITED STATES COURT OF APPEALS FOR THE NINTH CIRCUIT

REYNALDO GONZALEZ; THE ESTATE OF NOHEMI GONZALEZ; BEATRIZ GONZALEZ, INDIVIDUALLY AND AS ADMINISTRATOR OF THE ESTATE OF NOHEMI GONZALEZ; JOSE HERNANEZ; REY GONZALEZ; AND PAUL GONZALEZ,

Plaintiffs-Appellants,

v.

### GOOGLE, LLC,

Defendant-Appellee.

On Appeal from the United States District Court for the Northern District of California, No. 4:16-cv-3282 (DMR) Hon. Donna M. Ryu

# BRIEF OF AMICUS CURIAE ARTIFICIAL INTELLIGENCE LAW AND POLICY INSTITUTE IN SUPPORT OF REHEARING EN BANC

YAVAR BATHAEE BATHAEE DUNNE LLP 445 Park Avenue, 9th Floor New York, NY 10022 (332) 322-8835 yavar@bathaeedunne.com BRIAN J. DUNNE BATHAEE DUNNE LLP 633 West Fifth Street, 26th Floor Los Angeles, CA 90071 (213) 462-2277 bdunne@bathaeedunne.com

Attorneys for Amicus Curiae

August 9, 2021

Case: 18-16700, 08/09/2021, ID: 12196394, DktEntry: 91, Page 2 of 26

### CORPORATE DISCLOSURE STATEMENT

Amicus curiae Artificial Intelligence Law & Policy Institute is a not-forprofit, non-stock corporation. It has no parent corporation, and no publicly traded corporation has an ownership interest in it.

Date: August 9, 2021 BATHAEE DUNNE LLP

/s/ Brian J. Dunne
Brian J. Dunne
633 West Fifth Street, 26th Fl.
Los Angeles, CA 90071
(213) 462-2277
bdunne@bathaeedunne.com

Yavar Bathaee 445 Park Avenue, 9th Fl. New York, NY 10022 (332) 322-8835 yavar@bathaeedunne.com

Attorneys for Amicus Curiae Artificial Intelligence Law & Policy Institute

# TABLE OF CONTENTS

CORI	PORATE DISCLOSURE STATEMENT	i
TABI	LE OF AUTHORITIES	iii
INTE	REST OF AMICUS CURIAE	. 1
SUM	MARY OF ARGUMENT	. 3
ARG	UMENT	. 4
I.	IT IS AN ABSURD RESULT TO HOLD THAT SECTION 230 IMMUNIZES CONDUCT THAT AFFIRMATIVELY SURFACES, RATHER THAN BLOCKS OR SCREENS, OFFENSIVE MATERIAL	. 4
II.	THE PANEL DECISION PLAINLY RUNS AFOUL OF SECTION 230(E)(1), AS BARRING CIVIL REMEDIES FOR VIOLATIONS OF THE ANTI-TERRORISM ACT IMPAIRS THE ENFORCEMENT OF A FEDERAL CRIMINAL STATUTE.	10
III.	THE PANEL'S ANALYSIS OF GOOGLE'S ALGORITHMIC DECISIONMAKING MISUNDERSTANDS MODERN MACHINE LEARNING/AI TECHNOLOGY AND CREATES A LIABILITY VACUUM FOR ALGORITHMIC DECISIONS ATTRIBUTABLE TO IDENTIFIABLE ACTORS LIKE GOOGLE.	15
CON	CLUSION	19
CERT	ΓΙFICATE OF COMPLIANCE	20
CERT	ΓΙFICATE OF SERVICE	21

## **TABLE OF AUTHORITIES**

## Cases

Agency Holding Corp. v. Malley-Duff & Associates, Inc., 483 U.S. 143 (1987)14
Amalgamated Transit Union Local 1309, AFL-CIO v. Laidlaw Transit Services, Inc., 435 F.3d 1140 (9th Cir. 2006)
Amalgamated Transit Union Local 1309, AFL-CIO v. Laidlaw Transit Services, Inc., 448 F.3d 1092 (9th Cir. 2006)9
Barnes v. Yahoo, Inc., 570 F.3d 1096 (9th Cir. 2009)
Carafano v. Metrosplash.com, Inc., 339 F.3d 1119 (9th Cir. 2003)
Church of Scientology of Cal. v. U.S. Dep't of Justice, 612 F.2d 417 (9th Cir. 1979)11
Dyroff v. Ultimate Software Grp., Inc., 934 F.3d 1093 (9th Cir. 2019)
Fair Hous. Council of San Fernando Valley v. Roommates.com, LLC, 521 F.3d 1157 (9th Cir. 2008) (en banc)
Gonzalez v. Google LLC, 2 F.4th 871 (9th Cir. 2021)
United States v. Mays, 430 F.3d 963 (9th Cir. 2005)
Statutes and Legislative Materials
18 U.S.C. §§ 331-337

## **TABLE OF AUTHORITIES**

# **Statutes and Legislative Materials** (continued)

18 U.S.C. §§ 1001-1040
18 U.S.C. §§ 1091-1093
18 U.S.C. §§ 1961-1968
18 U.S.C. §§ 2331
18 U.S.C. § 2332
18 U.S.C. § 2332a-i
18 U.S.C. § 2333
18 U.S.C. §§ 401-403
47 U.S.C. § 230
S. Conf. Rep. 104-230 (1996)
Other Authorities
Yavar Bathaee, The Artificial Intelligence Black Box and the Failure of Intent and Causation,
31 Harv. J.L. & Tech. 889 (2018)
Yifat Nahmias and Maayan Perel, <i>The Oversight of Content Moderation by AI: Impact Assessments and Their Limitations</i> ,
58 HARV. J. ON LEGIS. 145 (2021)

### INTEREST OF AMICUS CURIAE<sup>1</sup>

The Artificial Intelligence Law and Policy Institute ("AILPI") is a not-for-profit organization that promotes equality and transparency in the digital community by educating the public regarding equality and transparency in technology, artificial intelligence, machine learning, and algorithmic fairness. AIPLI fosters discussion and spearheads policy analysis of the legal and social issues raised by these subjects and other important technology-related public policy matters. AIPLI conducts and participates in litigation in the public interest to preserve equality and transparency in technology and the digital community.

As part of its mission, AIPLI prepares and files amicus curiae briefs in cases with broad implications for the future of Americans' (and people the world over's) digital experience—cases like this one. The rapid, unchecked growth of powerful machine learning and algorithmic targeting technologies over the past half decade has transformed the modern Internet. Online content is, for all intents and purposes, now an infinite repository; one indexed, curated, and presented to users in digestible form by powerful algorithmic tools built and deployed by companies like Google.

<sup>&</sup>lt;sup>1</sup> All parties consent to the submission of this amicus brief. No counsel for a party has authored this brief in whole or in part, and no party, party's counsel, or any other person—other than amicus curiae and its counsel—has contributed money that was intended to fund preparing or submitting this brief. There is no relationship between AIPLI or its attorneys and petitioners or petitioners' counsel.

These content algorithms are not accidental, and they are not headless—they are designed to learn from data and to pursue defined objectives, and they control what human persons see, hear, and experience when they go online.

In this case, Google is alleged to have used its powerful targeting technology to affirmatively surface ISIS videos to users that Google's data tools determined would be particularly interested in ISIS videos. This is, according to the operative complaint in this matter, a violation of a federal criminal law—the Anti-Terrorism Act. Google, however, has argued that its algorithmic recommendation and surfacing of ISIS videos is "neutral" and "passive," and moreover that its conduct, even if it violates the Anti-Terrorism Act, is immunized by Section 230 of the Communications Decency Act. The panel below held that this was the case, and in doing so adopted as Ninth Circuit law some truly dangerous (and objectively wrong) interpretations of what Section 230 means, and how it interacts with other federal statutes and policies.

AILPI is concerned by the implications of the panel opinion in this case. However, AILPI also recognizes that the panel below believed that many of its holdings were required by this Court's precedent. Accordingly, AILPI respectfully submits that it is time for this circuit to revisit its Section 230 jurisprudence from the ground up—to forestall a decade of increasingly dystopian decisions given the growing role of algorithmic content technologies in the fabric of our everyday lives.

#### **SUMMARY OF ARGUMENT**

This is a case in which the panel decision is unambiguously wrong, with potentially wide-ranging—and deleterious—implications for the next decade of jurisprudence in this circuit. It is impossible to square the outcome below (in which Google's algorithmic recommendation of ISIS videos to persons likely to be interested in ISIS, in alleged contravention of the federal Anti-Terrorism Act, was held to be statutorily immunized by Section 230 of the Communications Decency Act) with the actual text and history of Section 230. There is, simply put, no reasonable *tabula rasa* reading of the Communications Decency Act in which Google's conduct, if proved, could be immunized from Anti-Terrorism Act liability by Section 230.

However, this is *also* a case (as multiple panel members expressly observed) in which much of the wrongness was foisted upon the panel below by this Court's precedent: to wit, more than a decade of creeping errors in the Ninth Circuit's Section 230 decisions, from *Carafano*, to *Roommates*, to *Kimzey*, to *Dyroff*—and many other opinions along the way. For nearly twenty years, this circuit has read into Section 230 mandates that are simply absent from the statutory text or history; has declined to seriously reckon with the meaning of Section 230(e) *et seq.*, both through its subparts and as a separately existing whole; and has applied an already unsupportable "test" in blindered ways that ignore the manner in which the

technology of the modern Internet, and particularly algorithmic decisionmaking, actually works. This needs to be corrected via *en banc* review. The alternative is to continue along an objectively incorrect interpretive path with respect to Section 230—one that does not properly give effect to unambiguous congressional intent—with a near-certainty of increasingly erroneous results in the Federal Reporter over the next several years.

The Gonzalez plaintiffs' petition presents a particularly appropriate vehicle for this circuit to convene *en banc* and right its interpretive wrongs with respect to Section 230. As set forth below, this case squarely presents three important, likely-to-recur interpretive problems with this circuit's Section 230 jurisprudence, each of which infected the panel decision below.

### **ARGUMENT**

I. IT IS AN ABSURD RESULT TO HOLD THAT SECTION 230 IMMUNIZES CONDUCT THAT AFFIRMATIVELY SURFACES, RATHER THAN BLOCKS OR SCREENS, OFFENSIVE MATERIAL.

The panel decision—purportedly applying this Court's decisions in *Carafano* v. *Metrosplash.com*, *Inc.*, 339 F.3d 1119 (9th Cir. 2003), *Fair Hous. Council of San Fernando Valley v. Roommates.com*, *LLC*, 521 F.3d 1157 (9th Cir. 2008) (en banc),<sup>2</sup>

<sup>&</sup>lt;sup>2</sup> This Court may overrule or clarify not just panel decisions like *Carafano* and *Dyroff*, but limited *en banc* decisions like *Roommates*, upon *en banc* rehearing of this case. *See*, *e.g.*, *U.S.* v. *Aguila-Montes de Oca*, 655 F.3d 915, 916-17 (9th Cir. 2011) (en banc) (overruling-in-part *Navarro-Lopez v. Gonzales*, 503 F.3d 1063 (9th

Kimzey v. Yelp!, Inc., 835 F.3d 1263 (9th Cir. 2016), and Dyroff v. Ultimate Software Grp., Inc., 934 F.3d 1093 (9th Cir. 2019)—determined that Google's algorithmic surfacing and recommendation of ISIS videos to users determined to be likely to be interested in ISIS videos (alleged in the Third Amended Complaint in Gonzalez at, for example, ¶¶ 534-55, see ER 182-85) was statutorily immunized by Section 230 of the Communications Decency Act. See Gonzalez v. Google LLC, 2 F.4th 871, 892-97 (9th Cir. 2021).

This was a perverse result given the unambiguous Congressional intent behind Section 230—to permit and incentivize *blocking and screening* of offensive material by service providers, in order to make the nascent Internet *less* of a morass of criminality and harassment, not more. *See, e.g.,* 47 U.S.C. § 230 ("Protection for private blocking and screening of offensive material"); *id.* § 230(c) ("Protection for 'Good Samaritan blocking and screening of offensive material"); *id.* § 230(b)(3) ("[It is the policy of the United States—] to encourage the development of technologies which maximize user control over what information is received by individuals, families, and schools who use the Internet and other interactive computer services; *id.* § 230(b)(4) ("[It is the policy of the United States—] to remove disincentives for the development and utilization of blocking and filtering

Cir. 2007) (en banc)), abrogated on other grounds by Descamps v. United States, 570 U.S. 254 (2013).

technologies that empower parents to restrict their children's access to objectionable or inappropriate online material"); *id.* § 230(b)(5) ("[It is the policy of the United States—] to ensure vigorous enforcement of Federal criminal laws to deter and punish trafficking in obscenity, stalking, and harassment by means of computer.").

As the Senate Conference Report explained section 230 immediately prior to its enactment:

The conference agreement adopts the House provision with minor modifications as a new section 230 of the Communications Act. This section provides "Good Samaritan" protections from civil liability for providers or users of an interactive computer service for actions to restrict or to enable restriction of access to objectionable online material. One of the specific purposes of this section is to overrule *Stratton-Oakmont v. Prodigy* and any other similar decisions which have treated such providers and users as publishers or speakers of content that is not their own because they have restricted access to objectionable material. The conferees believe that such decisions create serious obstacles to the important federal policy of empowering parents to determine the content of communications their children receive through interactive computer services.

S. Conf. Rep. 104-230 (1996), at p. 194 (emphasis added).

Yet despite all the above—words stacked on words stacked on words, from statutory text to authoritative legislative history—making indisputable that Congress passed Section 230, *including* its subsection (c)(1), to permit and incentivize "restrict[ing] access to objectionable material" in order to *keep Internet users safe*,

the panel decision here expressly holds that Section 230 immunizes conduct<sup>3</sup> by a service provider that *affirmatively surfaces* objectionable—and indeed, dangerously criminal—content and *targets* it to users who might be uniquely influenced by it. *See Gonzalez*, 2 F.4th at 892-97. Nothing in the text or structure of Section 230 compels this result; the bare language that one user or provider "shall not be treated as the publisher or speaker of any information provided by another information content provider" is, by its plain terms, irrelevant to whether Google has violated the Anti-Terrorism Act as alleged in the case below.

Nonetheless, the panel held that Section 230(c)(1) not only applies to the *opposite* of the behavior it was indisputably intended to encompass, but *immunizes* alleged violations of *federal anti-terrorism laws* by one of the world's largest and most powerful corporations, solely because of a creepingly-erroneous chain of decisions by this Court attempting to give effect to Section 230(c)(1) in various cases without ever revisiting first principles. It is time for a reboot.

To the extent the panel's holding was required by this Court's precedents in Carafano, Roommates, and/or Dyroff, those cases and their progeny must be

<sup>&</sup>lt;sup>3</sup> To the extent that Google has argued, and various prior decisions have held, that algorithmic surfacing and targeting of content is not "conduct" by the developer that creates and deploys such algorithms, this is a complete misapprehension of how machine learning, artificial intelligence, and algorithmic decisionmaking works on the modern Internet, as explained in greater detail in Section III of this amicus brief, *infra*.

overruled or limited so as to permit the unambiguously correct statutory result: that Section 230 does not immunize an Internet service provider's *affirmative surfacing* of offensive (and indeed, criminal) material. This can be done while still attempting to give effect to the words of Section 230(c)(1)—but this circuit's standard needs to take into account the purpose and structure of Section 230 as a whole, and most critically the section's unambiguously constrained scope (to enable *blocking and filtering*) and its separately-enumerated subsection, § 230(e) *et seq.*, that expressly defines Section 230's "Effect on other laws." 47 U.S.C. § 230(e)(1)-(5).

The interpretation of Section 230(c)(1) articulated by the panel below, which not only ignores the fact that Google's alleged conduct is the *direct logical opposite* of the conduct Section 230 was enacted to protect and incentivize, but repeatedly avoids rigorous engagement with Section 230(e) *et seq.*, despite that subsection's obvious pertinence to the issues here (*see, e.g., Gonzalez,* 2 F.4th at 890 (rebuffing argument § 230(e)(1) precludes § 230(c) immunity for Google's actions); *id.* at 891 n.9 (ignoring express distinctions between State and federal laws in the text of § 230(e) *et seq.* and in this Court's Section 230 decisions<sup>4</sup>)), is not a permissible method of statutory interpretation under this Court's precedent, given that it both ignores known Congressional intent and embraces an absurd result. *See, e.g.*,

<sup>&</sup>lt;sup>4</sup> See, e.g., Barnes v. Yahoo! Inc., 570 F.3d 1096, 1097 (9th Cir. 2009).

Amalgamated Transit Union Local 1309, AFL-CIO v. Laidlaw Transit Services, Inc., 435 F.3d 1140, 1145-46 (9th Cir. 2006) (holding that "less" means "more" based on a clearly expressed legislative intent from purpose and context).<sup>5</sup>

Here, there can be no dispute that the conduct alleged by the *Gonzalez* plaintiffs—that Google algorithmically recommends ISIS videos to users that Google has determined through data-mining and the application of machine-learning algorithms to be likely to be interested in ISIS videos (*see, e.g.,* ER 182-85 (TAC ¶¶ 534-55))—is not passive or neutral activity, but rather concrete action *by Google* to *surface and matchmake* videos promoting terrorism to persons determined by Google to be likely to be interested in videos promoting terrorism.

This is not an action by an Internet service provider to block or screen offensive conduct—it is the exact opposite. It is *content*, created, curated, and presented—tailored to the viewer—by machine-learning systems provided with mathematically discernable objectives by Google. Put simply, the algorithms create content for the viewer.

<sup>&</sup>lt;sup>5</sup> Even under the flip side of the coin, see Amalgamated Transit Union Local 1309, AFL-CIO v. Laidlaw Transit Services, Inc., 448 F.3d 1092, 1094-1100 (9th Cir. 2006) (Bybee, J., dissenting from denial of rehearing en banc), Google fares no better: the plain language of Section 230(c)(1) simply says that a provider "shall [not] be treated as the publisher or speaker of any information provided by another information content provider." It does not expressly preclude, limit, or immunize any sort of legal claim. In order to find such language in section 230 (aside from that in § 230(c)(2)), the Court must look to Section 230(e) ("Effect on other laws").

Whatever the precise sweep of Section 230(c) *et seq*.'s protections for providers of interactive computer services, the section cannot possibly encompass the *direct logical opposite* of the express reason that Congress promulgated it. There is no textual basis for this upside-down reading of Section 230(c), and all available sources of congressional intent behind the section affirmatively rule out such an interpretation. Yet this is what the panel below held—purportedly on constraint of this circuit's precedents. *En banc* review is required to prevent an absurd result.

II. THE PANEL DECISION PLAINLY RUNS AFOUL OF SECTION 230(E)(1), AS BARRING CIVIL REMEDIES FOR VIOLATIONS OF THE ANTI-TERRORISM ACT IMPAIRS THE ENFORCEMENT OF A FEDERAL CRIMINAL STATUTE.

In a single paragraph devoid of substantive analysis, the panel held that the Gonzalez plaintiffs' claims under the federal Anti-Terrorism Act could be barred by Section 230 despite an express provision, Section 230(e)(1), stating that "Nothing in this section shall be construed to impair the enforcement of . . . any . . . Federal criminal statute." *See Gonzalez*, 2 F.4th at 890. The basis for the panel's holding on this point was that Section 230(e)(1) "extends only to criminal prosecutions, and not civil actions based on criminal statutes." *Id.* The panel offered no actual substantive argument in favor of this holding; it simply cited to other circuit's decisions on that point, adopted the above "only . . . criminal prosecutions" holding on behalf of the Ninth Circuit, then moved along. The panel's decision on this incredibly important issue was wrong, with potentially widespread future implications not just for federal

Anti-Terrorism Act cases, but for cases brought under the federal Racketeer Influenced and Corrupt Organizations Act (RICO) as well.

First, the panel's holding that Section 230(e)(1) "extends only to criminal prosecutions" is nowhere in—and in fact, contrary to—the plain language of Section 230(e)(1): "Nothing in this section shall be construed to impair the enforcement of section 223 or 231 of this title, chapter 71 (relating to obscenity) or 110 (relating to sexual exploitation of children) of Title 18, or any other Federal criminal statute." The plain language of Section 230(e)(1) does not admit the additional requirement that the provision "extends only to criminal prosecutions"—especially since numerous federal criminal statutes, including the Anti-Terrorism Act itself—were expressly legislated by Congress to include multiple means of "enforcement." The "only ... criminal prosecutions" limitation adopted *ipse dixit* by the panel below is not in the statute—and it was error for the panel to add it. See Church of Scientology of Cal. v. U.S. Dep't of Justice, 612 F.2d 417, 421 (9th Cir. 1979) ("[I]n the vast majority of its legislation Congress does mean what it says and thus the statutory language is normally the best evidence of congressional intent.").

Second, there can be no serious dispute (although the panel decision essentially elides this point) that the Anti-Terrorism Act is a "federal criminal statute." The Anti-Terrorism Act comprises twenty-one statutory subsections codified as Chapter 113B within Part I of Title 18 of the United States Code. *See* 18

U.S.C. §§ 2331-2339d. Title 18 of the United States Code covers "Crimes and Criminal Procedure," and its Part I is titled, "Crimes." Within this statutory Part directed toward federal "Crimes," there are close to one hundred separate chapters, ranging from "Contempts" (Chapter 21, 18 U.S.C. §§ 401-403), to "Fraud and False Statements" (Chapter 47, 18 U.S.C. §§ 1001-1040), to "Genocide" (Chapter 50A, 18 U.S.C. §§ 1091-1093). All of the chapters within Part I of Title 18 define federal crimes (*see, e.g.,* Chapter 17—Coins and Currency, 18 U.S.C. §§ 331-337 (enumerating seven distinct federal crimes relating to coins and currency)), but some of the chapters in this Part also detail means of enforcement.

Two examples of the latter are Chapter 96—Racketeer Influenced and Corrupt Organizations (18 U.S.C. §§ 1961-1968), and Chapter 113B—Terrorism (18 U.S.C. §§ 2331-2339d). Each of these chapters—Chapter 96 and Chapter 113B—(1) expressly defines federal crimes (*see* 18 U.S.C. §§ 1961-1962 (RICO "Definitions" and "Prohibited Activities," respectively); 18 U.S.C. §§ 2331 and 2332a-2332i (Terrorism "Definitions" and prohibited activities, including "Use of Weapons of Mass Destruction," "Missile Systems Designed to Destroy Aircraft," and "Acts of Nuclear Terrorism"); (2) expressly specifies "Criminal Penalties" (*see* 18 U.S.C. § 1963 (RICO); 18 U.S.C. § 2332 (Terrorism)); and (3) expressly specifies "Civil Remedies" (*see* 18 U.S.C. § 1964 (RICO); 18 U.S.C. § 2333 (Terrorism)). The language of 18 U.S.C. § 2333(a), which was enacted after RICO, parallels that of 18

U.S.C. § 1964(c). There is no question based on structure, language, and context, that both RICO (Chapter 96 of Part I of Title 18) and the Anti-Terrorism Act (Chapter 113B of Part I of Title 18) are federal criminal statutes.

Next, the question under Section 230(e)(1) is whether precluding a lawsuit under the enumerated "Civil Remedies" provision of a federal criminal statute—for example, a RICO action under 18 U.S.C. § 1964 or an Anti-Terrorism Act action under 18 U.S.C. § 2333—"impairs the enforcement" of that federal criminal statute (*i.e.*, RICO or the Anti-Terrorism Act). The answer is self-evidently "yes" under basic, longstanding principles of statutory construction—the most obvious of which is that Congress is assumed to have done things for a reason, and Congress expressly designed certain federal criminal statutes in Part I of Title 18 (*e.g.*, Chapter 96—Racketeer Influenced and Corrupt Organizations Act, and Chapter 113B—Terrorism), to have enumerated "Criminal Penalties" *and* "Civil Remedies" provisions.

Congress may (indeed, must) be presumed to have legislated private enforcement of certain federal criminal statutes (e.g., RICO, the Anti-Terrorism Act), but not others (e.g., Coins and Currency), because Congress's avowed, intended scheme to enforce *certain* criminal statutes—including RICO and the Anti-Terrorism Act—extends beyond federal prosecutions. This is the only reasonable takeaway from the unique structure of Chapter 96—RICO and Chapter 113B—

Terrorism within Part I of Title 18. And it is a takeaway endorsed in the RICO context by the Supreme Court of the United States. See Agency Holding Corp. v. Malley-Duff & Associates, Inc., 483 U.S. 143, 151 (1987) (civil remedies under the Racketeer Influenced and Corrupt Organizations Act "bring to bear the pressure of 'private attorneys general' on a serious national problem for which public prosecutorial resources are deemed inadequate" (emphasis added)); cf. United States v. Mays, 430 F.3d 963, 965-67 (9th Cir. 2005) (discussing Congressional awareness and intent with respect to civil enforcement of criminal judgments: "By specifically importing the FDCPA's procedures into the MVRA, Congress clearly meant to make those procedures available in criminal cases.").

The panel decision ignored all of the above, instead holding without material analysis that "§ 230(e)(1)'s limitation on § 230 immunity extends only to criminal prosecutions . . . ." *Gonzalez*, 2 F.4th at 890. This was a serious error, with potentially far-reaching implications, including on federal RICO violations by purported interactive content providers.<sup>6</sup>

<sup>&</sup>lt;sup>6</sup> The panel recited, but did not analyze, the district court's statement about Section 230(e)(1) that "any ambiguity in the subsection's text was resolved by its title, "[n]o effect on criminal law." (*Id.* (citations omitted).) Aside from the fact that "[n]o effect on criminal law" doesn't actually resolve any interpretive issue—and aside from the fact that the language of 230(e)(1) is not, in fact, ambiguous—any interpretive methodology in which the titles of Section 230 subsections are accorded substantive weight in divining Congressional intent could not possibly support

Excising civil remedies from criminal statutory schemes cripples the scope of those statutes, and there is simply no evidence that Congress intended Section 230 to have such an effect. To the contrary, § 230(e)(1) evinces a clear intent not to displace criminal statutory schemes. Congress could have easily said it was referring to criminal prosecutions or actions brought by the government. It did not do so.

III. THE PANEL'S ANALYSIS OF GOOGLE'S ALGORITHMIC DECISIONMAKING MISUNDERSTANDS MODERN MACHINE LEARNING/AI TECHNOLOGY AND CREATES A LIABILITY VACUUM FOR ALGORITHMIC DECISIONS ATTRIBUTABLE TO IDENTIFIABLE ACTORS LIKE GOOGLE.

Finally, the panel's discussion and analysis—and the analysis of prior panel decisions from this circuit, most notably *Dyroff*—of the role that content algorithms play on the modern Internet, *see Gonzalez*, 2 F.4th at 892-97, is materially (and quite concerningly) inaccurate. Per the panel below, although the TAC in this case admittedly "alleges that Google recommends content—including ISIS videos—to users based upon users' viewing history and what is known about the users," *id.* at 894, that same TAC is purportedly "devoid of any allegations that Google specifically targeted ISIS content, or designed its website to encourage videos that further the terrorist group's mission," *id.* at 895. This is not an accurate

immunizing Google's alleged conduct here, given that the title of Section 230(c) is "Protection for 'Good Samaritan' blocking and screening of offensive material."

understanding of Google's powerful—and purpose-built, and carefully deployed—machine-learning technology.

Modern content surfacing, recommendation, and targeting algorithms like those alleged to have been deployed by Google in this case are not "websites" that are "neutral" to uploads. Rather, machine learning algorithmic tools like Google's carefully review and learn from each and every piece of content on Google's platform—and each and every action taken by a user on that platform—and then affirmatively surface particular content from a vast number of videos based on particular attributes.

These tools operate as designed, and learn as they do it. They are not bare "do this, then that" instructions, nor are they unknown or unknowable pieces of technology that operate in a vacuum. *See generally* Yavar Bathaee, *The Artificial Intelligence Black Box and the Failure of Intent and Causation*, 31 HARV. J.L. & TECH. 889, 897-906 (2018) (describing the development and operation of artificial intelligence technologies and machine-learning algorithms); *cf.* Yifat Nahmias and Maayan Perel, *The Oversight of Content Moderation by AI: Impact Assessments and Their Limitations*, 58 HARV. J. ON LEGIS. 145, 171-83 (2021) (discussing algorithmic

content moderation technologies deployed by YouTube and Facebook, among others).<sup>7</sup>

Contrary to the panel's assertion, "Google's algorithms [do not] function like traditional search engines that select particular content for users based on user inputs," Gonzalez, 2 F.4th at 897, and to hold Google immune from liability for the positive, programmed actions of its algorithmic tools based on this misunderstanding presages a troublesome liability vacuum over the next decade—because algorithms will be the primary way in which some of the world's largest and most pervasive companies (including Google and Facebook) interact with their users in the 2020s.

A holding by this circuit—the home base of both Google and Facebook, and the situs of forum selection clauses from both companies—that when users interact with algorithms designed and deployed by an Internet provider, the actions of those algorithms are not attributable to the provider who designed and deploys them, is incredibly problematic. And, the holding is based on a factual premise that has effectively been hardcoded in the law of this circuit—that machine-learning algorithms are mere facilitation tools, not means of creating user-tailored content. That factual error is at the very root of the panel's reasoning here, 2 F.4th at 892-97,

<sup>&</sup>lt;sup>7</sup> The TAC in this case alleges that Google affirmatively surfaces and targets ISIS content to users—not just that it fails to filter all of it. *See, e.g.,* ER 182-85 (TAC ¶¶ 534-55); *see also Gonzalez*, 2 F.4th at 892.

and is the hyper-factual centerpiece of this Court's 2019 panel decision in *Dyroff*, 934 F.3d at 1097-99. Given the centrality, importance, and recurrence of this Court's errors on this issue, *en banc* review is warranted to correct this circuit's treatment of algorithmic decisionmaking under Section 230 even separate from the other errors infecting the panel decision here.

### **CONCLUSION**

For the foregoing reasons, this Court should rehear this case *en banc* and hold that Section 230 of the Communications Decency Act does not immunize any of the *Gonzalez* plaintiffs' federal Anti-Terrorism Act claims.

Date: August 9, 2021 Respectfully submitted,

### **BATHAEE DUNNE LLP**

/s/ Brian J. Dunne
Brian J. Dunne
bdunne@bathaeedunne.com
633 W. Fifth Street, 26th Floor
Los Angeles, CA 90071
(213) 462-2277

Yavar Bathaee yavar@bathaeedunne.com Edward M. Grauman egrauman@bathaeedunne.com 445 Park Avenue, 9th Floor New York, NY 10022 (332) 205-7668

Attorneys for Amicus Curiae Artificial Intelligence Law & Policy Institute

## **CERTIFICATE OF COMPLIANCE**

# UNITED STATES COURT OF APPEALS FOR THE NINTH CIRCUIT

# Form 8. Certificate of Compliance for Briefs

Instructions for this form: <a href="http://www.ca9.uscourts.gov/forms/form08instructions.pdf">http://www.ca9.uscourts.gov/forms/form08instructions.pdf</a>

9th Cir. Case Number(s)18-16700
I am the attorney or self-represented party.
This brief contains 4198 words, excluding the items exempted by Fed. R. Ap
P. 32(f). The brief's type size and typeface comply with Fed. R. App. P. 32(a)(5) and (6).
I certify that this brief (select only one):
[ ] complies with the word limit of Cir. R. 32-1.
[ ] is a <b>cross-appeal</b> brief and complies with the word limit of Cir. R. 28.1-1.
[X] is an <b>amicus</b> brief and complies with the word limit of Fed. R. App. P. 29(a)(5), Cir. R. 29(c)(2), or Cir. R. 29-2(c)(3).
[ ] is for a <b>death penalty</b> case and complies with the word limit of Cir. R. 32-4.
[ ] complies with the longer length limit permitted by Cir. R. 32-2(b) because (select only one):     [ ] it is a joint brief submitted by separately represented parties;     [ ] a party or parties are filing a single brief in response to multiple briefs; or     [ ] a party or parties are filing a single brief in response to a longer joint brief.
[ ] complies with the length limit designated by court order dated
[ ] is accompanied by a motion to file a longer brief pursuant to Cir. R. 32-2(a).
Signature s/ Brian J. Dunne Date Aug. 9, 2021

Case: 18-16700, 08/09/2021, ID: 12196394, DktEntry: 91, Page 26 of 26

**CERTIFICATE OF SERVICE** 

I hereby certify that on this 9th day of August, 2021, I electronically filed the

foregoing with the Clerk of the Court for the United States Court of Appeals for the

Ninth Circuit using the appellate CM/ECF system. Counsel for all parties to the case

are registered CM/ECF users and will be served by the appellate CM/ECF system.

/s/ Brian J. Dunne

Brian J. Dunne

21